Department of Justice Canada | Ministère de la Justice Canada

NUMERO DU DOSSIER/FILE #:2016-000804
COTE DE SÉCURITÉ/SECURITY CLASSIFICATION: Protected B

TITRE/TITLE: Justice-Related Highlights Relevant to Pre-Inquiry Engagement Meeting Vancouver – Wednesday, January 13, 2016

SOMMAIRE EXÉCUTIF/EXECUTIVE SUMMARY

- The information contained in this note is intended to outline some of the current justice-related context for your pre-inquiry engagement meeting in Vancouver.

s.21(1)(a)
s.23

- [redacted]

- The information is intended to provide you with a general, high-level overview of some of the justice-related issues that have gained recent attention in media and other forums in the Vancouver, Vancouver Island, and Lower mainland area and may be raised during your pre-inquiry meeting.

- You will not be required to comment on any of these specific issues, but if you have any further questions or wish more information on any of these issues or any other issues raised during or surrounding the meetings, officials would be pleased to provide further information to you.

Soumis par (secteur)/Submitted by (Sector): Policy Sector

Responsable dans l'équipe du SM/Lead in the DM Team: Sarah Geh

Revue dans l'ULM par/Edited in the MLU by: Matt Ignatowicz

Soumis au CM/Submitted to MO:

Department of Justice Canada | Ministère de la Justice Canada

Protected B
FOR INFORMATION

2016-000804

MEMORANDUM FOR THE MINISTER

Justice-Related Highlights Relevant to Pre-Inquiry Engagement Meeting – Vancouver – Wednesday, January 13, 2016

ISSUE

The information below is intended to outline some of the current justice-related context for your pre-inquiry engagement meeting in Vancouver.

BACKGROUND

s.21(1)(a)

s.23

[redacted] The information below is intended to provide you with a general, high-level overview of some of the issues that have gained recent attention in media and other forums and so may be raised. Hyperlinks have been included only for your quick reference, if needed.

Recent media coverage –

- Disproportionate numbers of missing and murdered Aboriginal women are from BC http://www.vancouversun.com/news/many+missing+murdered+aboriginal+women+from/11490141/story.html
- Disagreement over the implementation by the Government of British Columbia of recommendations of the Missing Women Commission of Inquiry http://www.huffingtonpost.ca/2014/12/04/bc-missing-women-report_n_6272146.html?utm_hp_ref=highway-of-tears
- West Coast LEAF assesses B.C. government action as failing Indigenous women http://vancouver.24hrs.ca/2015/11/02/bc-failing-aboriginal-women-group
- Serial killers prey on Indigenous women http://www.theglobeandmail.com/news/national/prime-targets-serial-killers-and-indigenous-women/article27435090/

Recent high profile deaths and disappearances –

- CBC has reported on a number of individuals deaths and disappearances, including many in the Downtown Eastside – http://www2.gov.bc.ca/gov/content/justice/about-bcs-justice-system/recent-inquiries
- Samantha Paul (Tk'emlúps te Secwépemc – remains found near Kamloops 2014 – outstanding investigation) http://www.kamloopsthisweek.com/almost-a-year-later-samantha-paul-case-remains-a-mystery/
- Crystal Paul (charges laid in 2015) http://www.cbc.ca/news/canada/british-columbia/daniel-alphonse-paul-charged-with-2nd-degree-murder-of-crystal-paul-1.3144211

- Cady Quaw (charges laid in 2015) http://www.vancitybuzz.com/2015/05/gordon-alexander-david-arrested-manslaughter/
- Delores Brown (Hul'qumi'num Treaty Group – remains found off Norway Island 2015 – outstanding investigation)) http://vancouverisland.ctvnews.ca/remains-found-off-b-c-island-those-of-missing-19-year-old-1.2533091
- Paige (2015 child welfare report on death – Downtown Eastside) http://www.cbc.ca/news/canada/british-columbia/death-of-b-c-aboriginal-teen-paige-under-rcmp-investigation-1.3234158
- Jennifer McPherson (remains found near Alert Bay 2013 – conviction 2014) http://www.theglobeandmail.com/news/national/convicted-wife-killer-admits-to-murder-of-second-woman-nine-years-ago/article26092887/
- Roxanne Louie (Osoyoos Indian Band – remains found near Penticton 2014 – outstanding investigation) http://www.bclocalnews.com/news/364580681.html?mobile=true
- Summer Star Elizabeth Krista-Lee (CJ) Fowler (Gitanamaax First Nation – remains found near Kamloops 2012 – conviction 2015) http://www.canada.com/news/after+teen+murder+assembly+first+nations+renews+call+inquiry+hundreds+cases/7678021/story.html; http://www.cbc.ca/news/canada/british-columbia/taylor-murder-trial-cj-fowler-convicted-1.3271628
- Elizabeth Marie Lagis (remains found near Black Creek 2012 – investigation outstanding) http://www.campbellrivermirror.com/news/142092483.html

Local front-line organizations working with family members / Stakeholder coalition –

- The 29-member Coalition on Missing and Murdered Indigenous Women and Girls includes most of the relevant First Nations and non-governmental organizations in British Columbia – http://www.amnesty.ca/sites/amnesty/files/2015Nov09_CoalitionPRandBackgrounders_ActionMMIWG_Combined.pdf

Relevant earlier inquiries / international report –

- 2011 report of the Vancouver Police Department *We Can Do Better* (http://vancouver.ca/police/assets/pdf/reports-policies/missing-murdered-aboriginal-women-canada-report.pdf)
- 2012 Missing Women Commission of Inquiry (Oppal Commission) issued the report *Forsaken* – there have been two updates on implementation by the Government of BC – http://www2.gov.bc.ca/gov/content/justice/about-bcs-justice-system/recent-inquiries
- *Blueprint for an Inquiry: Learning from the Failures of the Missing Women Commission of Inquiry* issued by a Coalition of Legal non-governmental groups with recommendations for any future inquiry https://bccla.org/wp-content/uploads/2012/11/20121119-Report-Missing-Women-Inquiry.pdf
- 2014 report by the Inter-American Commission on Human Rights *Missing and Murdered Indigenous Women and Girls in British Columbia, Canada* made a number of recommendations – http://www.oas.org/en/iachr/reports/pdfs/Indigenous-Women-BC-Canada-en.pdf

Local policing highlights –

- 2001 – Project Evenhanded (a joint RCMP and Vancouver Police task force) was set up to investigate some 68 missing and/or murdered women from the Downtown Eastside of Vancouver and the surrounding areas
- 2013 – Martin Tremblay found guilty of overdose deaths of two girls (Vancouver Downtown Eastside), and ruled dangerous offender 2015
- 2007 – Robert Pickton convicted of the deaths of six women – he was charged with first-degree murder in 26 deaths, DNA evidence was found at his farm in connection with 33 deaths, and he at one time claimed to have killed 49 women
- 1988 – Gilbert Paul Jordan convicted of death of one woman – suspected in deaths of four others
- 1982 – Clifford Olsen pled guilty in deaths of 11 children, including one Métis girl.

s.21(1)(a)
s.23

[redacted]

CONSIDERATIONS

Together, these issues provide a general, high-level overview of some of the justice-related context for the Vancouver pre-inquiry engagement meeting. You will not be required to comment on any of these specific issues, but if you have any further questions or wish more information on any of these issues or any other issues raised during or surrounding the meetings, officials would be pleased to provide further information to you.

CONCLUSION

The information contained in this note is intended to provide you with a general, high-level overview of some of the justice-related issues that have gained recent attention in media and other forums in the Vancouver, Vancouver Island, and Lower mainland area and so may be raised during your pre-inquiry meeting.

ANNEXES

Annex 1: Media Articles

PREPARED BY
Lisa M. Hitch
Senior Counsel
Family, Children and Youth Section
613-941-2336

Pages 6 to / à 13

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(e)

of the Access to Information Act

de la Loi sur l'accès à l'information

Department of Justice Canada | Ministère de la Justice Canada

CCM#: 2016-001015
Secret
For Information

MEMORANDUM TO THE DEPUTY MINISTER

Deputy Ministers' Committee on Cyber Security
January 26, 2016, 9:30-11:30 a.m., 269 Laurier Ave. W. 19th Fl. Executive Boardroom
(BRIEFING NOTE FOR MEETING)

SUMMARY

- Deputy Ministers are expected to be apprised of cyber security mandate commitments and options for proceedings with a cyber security review.

BACKGROUND

The following items are on the Agenda, *Annex A*, in addition to *Opening Remarks* and *Roundtable*:

1) Cyber Security Mandate Commitments

The Deputy Minister of Public Safety will lead a discussion of his Minister's Mandate Letter commitment that he "lead a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats" ("the Review") in collaboration with the Ministers of National Defence, Infrastructure and Communities, of Public Services and Procurement and of Innovation, Science and Economic Development and the President of the Treasury Board."

The Deputy Minister is expected to precede the discussion with the presentation of a short deck. The deck is to set out the broad objectives of the Review, namely to conduct a credible and comprehensive stakeholder consultation, identify gaps and related solutions and innovative measures, advance a positive as opposed to reactive stance towards cyber security and position Government to reap the benefits while addressing the challenges of the digital age. The vision for cyberspace being proposed focuses on promoting fundamental rights and freedoms, market access, building cyber resilience of critical infrastructure and developing economic growth and fostering cross-cutting partnerships and collaboration.

A Cyber Security Review Working Group is preparing the following documents expected for early February 2016: 1) *Review Framing Document*, identifying key challenges and themes that should be addressed; 2) a *Stakeholder Chart*, listing key stakeholders and anticipated issues related to the Review and 3) *Options for Conducting the Review*, outlining potential scope and timelines.

2) RCMP Cyber Related Initiatives

Deputy Commissioner Henschel is expected to briefly present the *RCMP's Cybercrime Strategy* ("Strategy"), *Annex B*, released December 2, 2015. The Strategy sets out an operational framework and an action plan to help the RCMP reduce the threat and impact of cybercrime in Canada. The operational framework is supported by three pillars that will guide the RCMP's efforts:

1. identifying and prioritizing cybercrime threats through intelligence collection and analysis;
2. pursuing cybercrime through targeted enforcement and investigative action; and
3. supporting cybercrime investigations with specialized skills, tools and training.

A 15-point action plan is to be implemented by 2020. Action items include:

- creating a new investigative team dedicated to combating high-priority cybercrime;
- establishing a dedicated intelligence unit to identify new and emerging cybercrime threats;
- improving digital forensic evidence capabilities for cybercrime investigations; and
- expanding training opportunities for Canadian law enforcement in relation to cybercrime.

s.21(1)(a)
s.21(1)(b)

[redacted]

3) Recent Cyber Security Developments Deck

The *Update on Recent Cyber Security Developments Deck*, *Annex C*, at page 6 mentions the invalidation of the U.S. Safe Harbour Agreement. The invalidation resulted from the October 6, 2015 decision of the Court of Justice of the European Union in *Schrems*.

s.23

[redacted]

s.23

[redacted]

DISCUSSION

Cyber Security Review

s.21(1)(a)

s.21(1)(b)

s.69(1)(g) re (c)

[redacted]

Cyber security was an agenda item on the Meeting of FPT Ministers Responsible for Justice and Public Safety held in Québec City on January 21, 2016. [redacted]

CCM#: 2016-0010 [redacted]

s.21(1)(a)
s.21(1)(b)
s.23
s.69(1)(g) re (c)

[redacted]

RESOURCE IMPLICATIONS

N/A

COMMUNICATION IMPLICATIONS

N/A

NEXT STEPS

Updates on key legal issues and advice related to the initiatives mentioned will be brought to your attention.

Attachments: 5

Annex A: Agenda
Annex B: The RCMP Cybercrime Strategy
Annex C: Update on Recent Cyber Security Developments Deck
Annex D: [redacted]
Annex E: [redacted]

CCM#: 2016-001015

Prepared by:
Anna Colaianni, Counsel, PSDI, (613-952-4731)
Date: January 22, 2016

Reviewed by:
Michael W. Duffy, Senior General Counsel, PSDI, (613-960-0880)
Date: January 22, 2016

Approved by:
Elisabeth Eid, Assistant Deputy Attorney General, PSDI, (613-952-4774)
Date: January 22, 2016

Comité des Sous-ministres sur la cybersécurité

26 janvier 2016 – de 9 h 30 à 11 h 00
269, avenue Laurier Ouest, salle de conférence du 19e étage

ORDRE DU JOUR

Heure	Point	Documentation associée
1. 9 h 30 – 9 h 35 *(5 min)*	**Mot de bienvenue** François Guimont, Sous-ministre Sécurité publique Canada	S.O.
2. 9 h 35 - 10 h 15 (40 *min)*	**Engagements du mandat sur la Cybersécurité** François Guimont et les sous-ministres responsables, Sécurité publique Canada et les ministères responsables *Pour discussion : Discussion stratégique sur les points du mandat. En particulier, les options pour faire un examen de la cybersécurité dirigé par le ministre de la Sécurité publique.*	S.O.
3. 10 h 15 - 10 h 30 (15 *min)*	**La Stratégie de lutte contre la cybercriminalité de la GRC** Bob Paulson, commissaire, Gendarmerie royale du Canada (GRC) *À titre d'information : Une présentation sur la Stratégie de lutte contre la cybercriminalité de la GRC et les initiatives qui sont liées à la cybernétique.*	Les documents seront distribués avant ou pendant la réunion.
4. 10 h 30 - 10 h 50 (20 *min)*	**Présentation de l'invité spéciale: Cyber sécurité dans le secteur de l'énergie** Bob Hamilton, Sous-ministre Ressources naturelles Canada *Pour discussion : Une présentation de Ressources naturelles Canada sur la cyber-sécurité dans le secteur de l'énergie.*	Les documents seront distribués avant ou pendant la réunion.
5. 10 h 50 – 11 h 00 *(10 min)*	**Tour de table et la répartition des développements récents en matière de cybersécurité** Monik Beauregard, sous-ministre adjointe principale Sécurité publique Canada *Pour information : Examen des derniers développements et évènements de l'ensemble du gouvernement en matière de cybersécurité.*	Les documents seront distribués avant ou pendant la réunion.

ANNEX A

Deputy Ministers' Committee on Cyber Security

January 26, 2016 – 9:30 to 11:00 a.m.
19th floor, Executive Boardroom, 269 Laurier Avenue West
(1.5 hours)

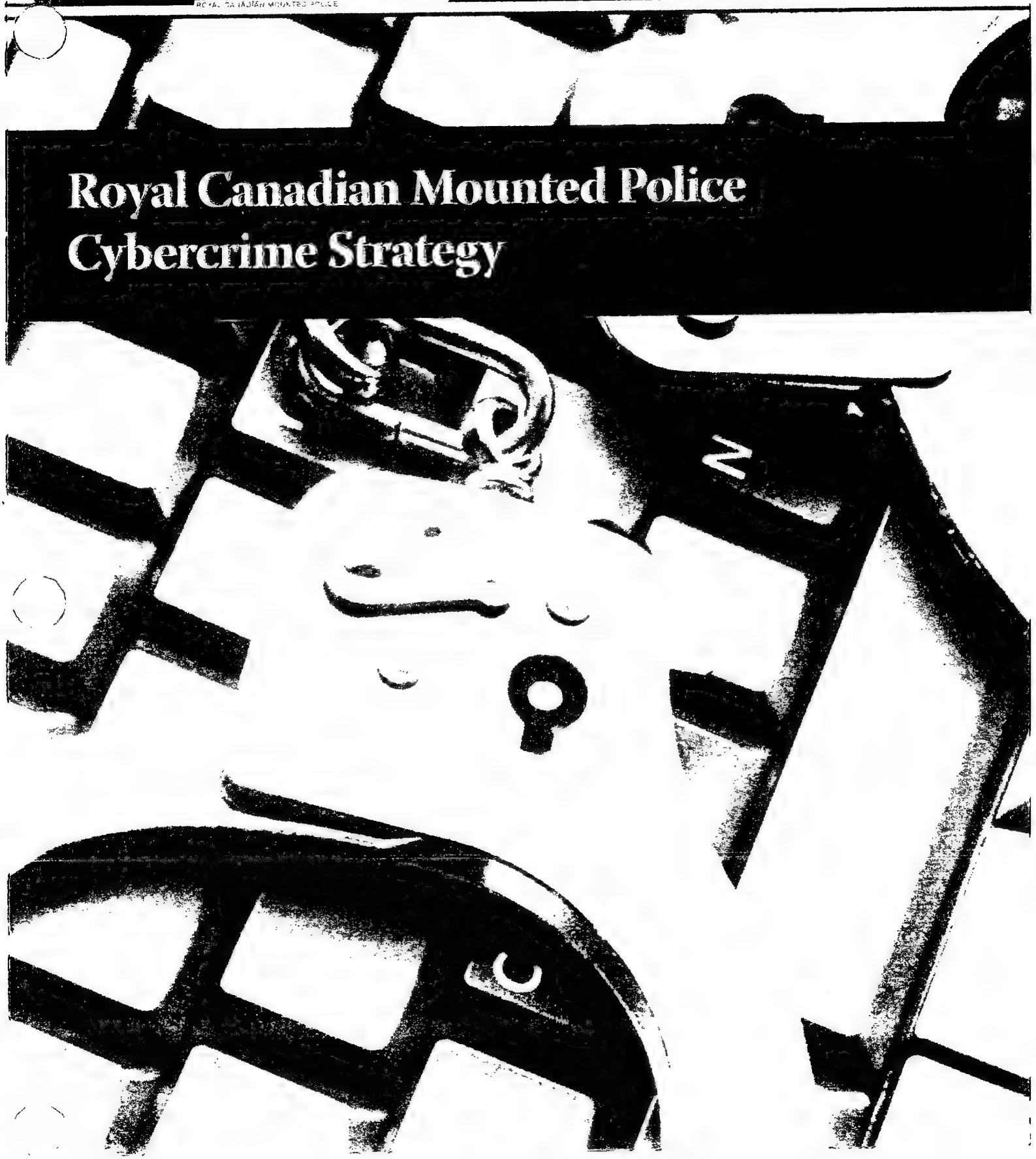
AGENDA

Time	Item	Associated Documentation
1. 9:30-9:35 *(5 mins)*	**Opening Remarks** François Guimont, Deputy Minister, Public Safety Canada	N/A
2. 9:35-10:15 *(40 mins)*	**Cyber Security Mandate Commitments** François Guimont, Deputy Minister et al., Public Safety Canada et al. *For discussion: A strategic discussion on mandate items. In particular, options to roll out a cyber security review led by the Minister of Public Safety and Emergency Preparedness.*	Documents will be distributed prior to or at the meeting.
3. 10:15-10:30 (15 *mins)*	**RCMP Cyber Related Initiatives** Bob Paulson, Commissioner, Royal Canadian Mounted Police (RCMP) *For information: A presentation on the RCMP Cybercrime Strategy and supporting cyber-related initiatives.*	Documents will be distributed prior to or at the meeting
4. 10:30-10:50 (20 *mins)*	**Special Guest Presentation: Cyber Security in the Energy Sector** Bob Hamilton, Deputy Minister Natural Resources Canada *For discussion: A presentation from Natural Resources Canada on cyber security in the energy sector.*	Documents will be distributed prior to or at the meeting.
5. 10:50-11:00 *(10 mins)*	**Roundtable and Distribution of the Recent Cyber Developments Deck** Monik Beauregard, Senior Assistant Deputy Minister Public Safety Canada *For information: Review of cyber-related developments and events from across Government*	Documents will be distributed prior to or at the meeting.

ANNEX B

RCMP
ROYAL CANADIAN MOUNTED POLICE

Royal Canadian Mounted Police Cybercrime Strategy



Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Executive Summary

In 2010, the Government of Canada launched *Canada's Cyber Security Strategy* to protect Canadian governments, businesses, critical infrastructure and citizens from cyber threats. The Strategy helped shape Canada's knowledge of cyber technology and guides Canada's efforts in securing government and other vital systems, and protecting Canadians online.

Consistent with the government's efforts to make cyberspace more secure for all Canadians, the RCMP *Cybercrime Strategy* is based on extensive internal and external consultation and focuses on ways to improve Canada's national police force in its fight against the rising and evolving threat of cybercrime. This strategy complements *Canada's Cyber Security Strategy* to help keep Canadians secure online.

The RCMP has a broad mandate when it comes to investigating and apprehending criminals in the online world, or otherwise disrupting cybercrime activity. The *RCMP Cybercrime Strategy* is therefore broad in scope and reflects the role of cyber in several law enforcement areas. The *RCMP Cybercrime Strategy's* vision is to reduce the threat, impact and victimization of cybercrime in Canada through law enforcement action. The following three pillars are identified within the strategy to guide the RCMP's efforts in combating cybercrime:

- Identify and prioritize cybercrime threats through intelligence collection and analysis;
- Pursue cybercrime through targeted enforcement and investigative action; and,
- Support cybercrime investigations with specialized skills, tools and training.

The *RCMP Cybercrime Strategy* sets out in an Operational Framework and a supporting Action Plan, objectives, strategic enablers and 15 action items, which the RCMP will implement over the next five years and beyond. Collectively, these initiatives will enable Canada's national police force to better combat cybercrime in concert with its domestic and international law enforcement partners and other stakeholders.

Table of Contents

Cybercrime requires new ways of policing

Cybercrime is on the rise, both in Canada and internationally.

Once considered the domain of individuals with specialized skills, cybercrime has expanded to other offenders as the requisite technical know-how becomes more accessible. Widely available and ready-made malicious software ('malware') and online cybercrime-for-hire services provide criminals with new and simplified ways to steal and exchange sensitive and personal information. As a result, criminals are constantly looking for vulnerabilities in new technologies that may be exploited for unlawful purposes, and new ways to victimize public and private sector organizations and Canadian citizens who rely on these technologies.

Cybercrime threats range in scope and impact. On a personal level, cybercrimes may target individuals through online scams or other fraudulent techniques. Cybercrimes may come with other social costs and devastating forms of victimization, such as online child sexual exploitation or the rising prevalence of cyber bullying. Cybercrime threats are also facilitated by organized crime networks and cause significant economic losses to Canadian businesses and citizens. On a commercial level, these threats target financial institutions, large-scale retailers and other organizations to steal personal consumer information, such as online passwords and credit card information, or to gain insider knowledge on intellectual property or trade secrets. On a national security level, state-sponsored and other criminal threat actors use sophisticated and covert cyber capabilities to perform espionage, steal sensitive information or to potentially conduct more disruptive attacks against Canada's critical infrastructure and other vital cyber systems.

The criminal exploitation of new and emerging technologies requires new policing measures to keep pace in a digital era. The same technologies that people and organizations use for legitimate purposes may be used by criminals to mask their online activities and evade detection from law enforcement. Police must often find technical solutions to decrypt, unlock or otherwise deal with encryption technologies, re-routed Internet Protocol (IP) addresses and other technical roadblocks that criminals exploit to cover their digital tracks and commit cybercrimes. Criminal activities in cyberspace are also complex and often transnational in character, where potential evidence is transient and spread across multiple jurisdictions.

To varying degrees, cybercrimes affect Canadians in real and harmful ways. For law enforcement, addressing cybercrime requires broad-based domestic and international police cooperation, engagement with public and private sector organizations, and integrating new technical skills and tools with traditional enforcement measures. As Canada's national police force, the RCMP must strive to be a leader in combating cybercrime. The following strategy and action plan demonstrates the RCMP's continued commitment against cybercrime.

Defining cybercrime

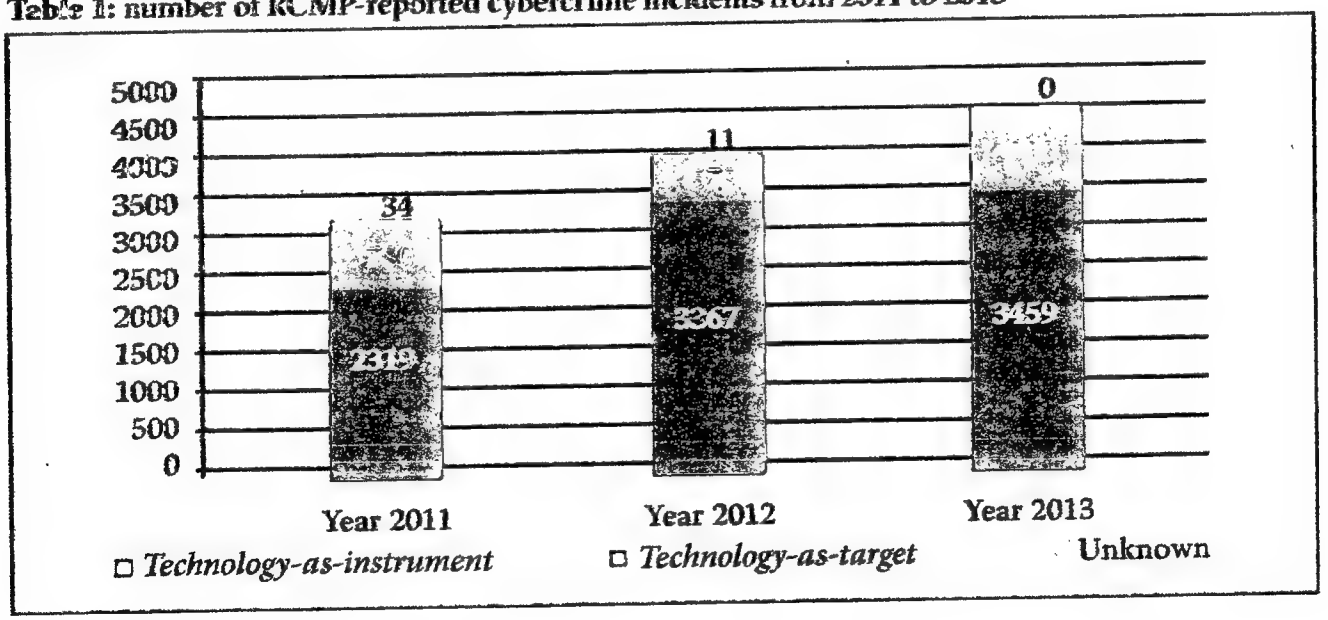
The RCMP interprets cybercrime to be any crime where cyber - the Internet and information technologies, such as computers, tablets, personal digital assistants or mobile devices - has a substantial role in the commission of a criminal offence. Under this broad lens, the RCMP breaks cybercrime into two categories:

- *technology-as-target* - criminal offences targeting computers and other information technologies, such as those involving the unauthorized use of computers or mischief in relation to data, and;
- *technology-as-instrument* - criminal offences where the Internet and information technologies are instrumental in the commission of a crime, such as those involving fraud, identity theft, intellectual property infringements, money laundering, drug trafficking, human trafficking, organized crime or terrorist activities, child sexual exploitation or cyber bullying.

Prevalence of cybercrime

RCMP statistics suggest that cybercrime is increasing in Canada. In 2013, the RCMP received over 4,400 reported incidents of cybercrime: an increase of more than 40% (over 1,300 reported incidents) from 2011. The majority of reported cybercrime incidents involve *technology-as-instrument* offences, but reported cybercrime incidents involving *technology-as-target* offences are on the rise. In a small number of reported cybercrime incidents, the type of offence could not be determined as either *technology-as-instrument* or *technology-as-target* (i.e. Unknown).

Table 1: number of RCMP-reported cybercrime incidents from 2011 to 2013



Additional information on cybercrime

Additional information on cybercrime, including expanded definitions and select case studies, may be found in the RCMP's first public report on cybercrime, Cybercrime: an overview of incidents and issues in Canada (available online at: http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.htm).

The RCMP's approach to combating cybercrime

The RCMP is the only federal organization with the mandate and authority to investigate criminal offences related to cybercrime, such as those targeting government systems and networks, or other critical infrastructure sectors. Criminal intelligence allows law enforcement to 'connect the dots' of information from local to national and international criminal activity. As Canada's national police force, the RCMP has a broad mandate to investigate criminals in the cyber realm, resulting in their apprehension or otherwise disrupting their cybercrime activity. Law enforcement activities extend from identifying and prioritizing cybercrime threats based on criminal intelligence, to investigating and disrupting cybercrime activities, to handling digital evidence in support of cybercrime investigations.

The RCMP's cyber-related roles and responsibilities align with its duty to preserve the peace and prevent crime and other offences against Canadian law as outlined in the *Royal Canadian Mounted Police Act*. Where the RCMP has been contracted as the local police service of jurisdiction at provincial, territorial and municipal levels, it also has a broad policing mandate in matters related to cybercrime as many crimes are committed by way of modern technologies.

The RCMP also has a pivotal role within the broader government's cyber community. Under *Canada's Cyber Security Strategy*, the RCMP works closely with its government partners to foster a safe and secure cyber environment in Canada.

The following section organizes the RCMP's cyber-related roles and responsibilities around three main areas: criminal intelligence, criminal investigations and specialized services.

Criminal intelligence

The RCMP takes an intelligence-led approach to policing. Criminal intelligence allows law enforcement to 'connect the dots' of information from local to national and international criminal activity. Whether tactical, operational or strategic, criminal intelligence enables the RCMP and other Canadian police forces to set priorities and allocate resources based on the most significant criminal threats to Canada. This concept also applies to cybercrime, especially given its transnational dimension and the inherent need to identify patterns and relationships between cybercrime data and other relevant data sources from multiple jurisdictions.

The RCMP may investigate cybercrime in response to a complaint or proactively as a result of criminal intelligence. Cybercrime intelligence - coming from investigations, police information databases, open source research and analysis, or partner collaboration between law enforcement and public and private sector stakeholders - can identify prolific and serious offenders in cyberspace and may objectively direct police resources to major cybercrime targets. The RCMP analyzes criminal intelligence from a wide array of sources, identifies emerging cybercrime threats, and makes links between cybercrime and other criminal domains, such as organized crime or financial crime.

Operational centres

Canadian Anti-Fraud Centre

The Canadian Anti-Fraud Centre (CAFC) is Canada's trusted source for reporting and mitigating online mass marketing fraud. It is a partnership among the RCMP, Ontario Provincial Police (OPP) and the Competition Bureau. In 2014, the CAFC received over 14,000 complaints of cyber-related fraud (email and website scams), accounting for more than $45 million in reported losses. Additional information may be found at: www.antifraudcentre-centreantifraude.ca.

National Child Exploitation Coordination Centre

The RCMP National Child Exploitation Coordination Centre (NCECC) works with law enforcement partners, government agencies, non-government organizations and industry stakeholders across Canada and internationally to combat the online sexual exploitation of children. The NCECC also works closely with the Canadian Centre for Child Protection, an organization that operates Canada's national tipline (www.cybertip.ca) for reporting the online sexual exploitation of children. In 2014, the NCECC received nearly 3,500 reported incidents and requests for assistance from law enforcement and other partners concerning online child sexual exploitation.

Criminal investigations

At the federal level, the RCMP investigates serious and organized crime, economic crime, a range of **national security threats, and enforces Federal statutes. These investigations may extend to federal offences involving suspected cybercrime activities, such as money laundering and terrorist financing,** market fraud, threats to Canada's critical infrastructure, intellectual property infringements or drug **trafficking. The RCMP works in concert with domestic and international law enforcement partners** and other stakeholders to combat cybercrime threats that cross jurisdictional boundaries and require joint force operations.

International policing plays a pivotal role in the RCMP's response to cybercrime. Cybercrime is often **transnational, where a perpetrator in one country can affect victims in many others. As evidence of criminal activity may easily flow across national borders in cyberspace, the RCMP must work with** multilateral partners to obtain and analyze evidence, which is enabled by police-to-police information sharing and formal legal mechanisms. Given the borderless nature of cybercrime, the RCMP works closely with its domestic and international law enforcement partners, and other stakeholders in both public and private sectors, to address common cybercrime threats through various enforcement measures, leading to arrests and charges or other disruption outcomes.

Through contract policing services, the RCMP plays a significant role in addressing cybercrime in contracted provinces, territories and municipalities. Law enforcement activities in these jurisdictions **extend to a range of criminal offences where the Internet and related technologies play an integral role, such as online child sexual exploitation, local and regional types of fraud, or various offences** associated with cyber bullying.

Specialized Services

The RCMP's specialized and technological services play a critical role in cybercrime investigations. Cybercrime often involves surreptitious online activity, where the right law enforcement skills and tools are required to attribute cybercrime activity to a source, identify possible suspects and handle high volumes of digital evidence, such as terabytes of data from lawfully seized computers, hard **drives and mobile devices. Cybercrime investigations differ significantly from traditional criminal investigations. They have a greater requirement for operating in online environments through open** source analysis and covert means, and obtaining and analyzing data - and potential digital evidence **- to drive investigations. This work is critical to criminal investigations with cyber elements, and will** increase in complexity and volume as criminals continue to exploit new and emerging technologies.

The RCMP Technical Investigation Services (TIS) is a key part of the RCMP's specialized services for cybercrime investigations. The TIS provides technical domain expertise and digital forensic services to cybercrime investigations to all levels of policing in Canada, in addition to those involving international **policing. The TIS maintains expertise in the forensic investigation of computers and networks, and** provides other specialized services, such as expert testimony in criminal court proceedings involving **cybercrime investigations. The RCMP Integrated Technological Crime Units (ITCUs) also provide** specialized services to cybercrime investigations. ITCUs are strategically located across Canada to respond to cybercrime incidents in collaboration with other domestic and international police services, and often lead cybercrime investigations on behalf of Canada that are national or international in scope. **These units also process and analyze digital evidence in support of cybercrime and other criminal** investigations, which may involve computer forensics, network systems analysis, data recovery and retrieval, malware reverse engineering, and acquiring operational tools in support of cybercrime investigative techniques.

The RCMP's specialized services also extend to equipping law enforcement with the right training and skills to combat cybercrime. Cybercrime investigations require basic and advanced training to keep pace with criminals in cyberspace. As part of its National Police Services, the RCMP, through the Canadian Police College, provides law enforcement training and educational opportunities on **cybercrime investigations and intelligence gathering. The National Police Services are a coordinated** and integrated series of programs and services accessible to Canadian law enforcement that assist in the investigation of crime, including cybercrime.

RCMP Cybercrime Operational Framework

The RCMP Cybercrime Operational Framework is designed to capture the RCMP's vision, pillars, objectives and strategic enablers to combat cybercrime, which cascade throughout the action plan in **the next section. The framework and action plan centre on core policing operations in the cyber realm,** and equipping the RCMP with the right people, skills and tools in a digital era.

RCMP Cybercrime Operational Framework			
Vision – Reduce the threat, impact and victimization of cybercrime in Canada			
(P) PILLARS	Identify and prioritize cybercrime threats through intelligence collection and analysis (**P1**)	Pursue cybercrime through targeted enforcement and investigative action (**P2**)	Support cybercrime investigations with specialized skills, tools and training (**P3**)
(O) OBJECTIVES	• Strengthen the collection and analysis of cybercrime data to drive investigations and other policing measures (**O1**) • Exploit intelligence to identify serious cybercrime threats and deny cybercriminals of their tools (**O2**) • Work with law enforcement and industry to tactically disrupt national and international cybercrime threats (O3)	• Develop a highly trained team for priority cybercrime investigations (**O4**) • Expand technical capabilities to augment investigations where cyber is integral to a suspected criminal offence (**O5**) • Target the most sophisticated and complex cybercrimes in concert with domestic and international partners (**O6**)	• Expand capabilities to handle digital evidence in support of cybercrime investigations (**O7**) • Acquire new operational tools for cyber-related investigations (**O8**) • Expand law enforcement training for cybercrime investigators and intelligence analysts (**O9**)
(E) ENABLERS	Skills– **Develop a robust and scalable law enforcement training regime to more effectively** address cybercrime (E1) Tools– Equip law enforcement with the operational tools they need to investigate cybercrime at all levels of policing (E2) Information Sharing– Make it easier for victims to report cybercrime and improve information sharing between partners (E3) Coordination – **Enable joint force operations and deconfliction with law enforcement partners** when targeting cybercrime (E4) Industry – **Engage industry to address shared cybercrime issues and foster mutually beneficial** relationships (E5) Community Awareness – Inform Canadians and industry of new and emerging threats to help prevent cybercrime at the onset (E6) Legislation and Policy– Support the modernization of Canada's legal tools to keep pace with technological change (E7)		

RCMP Action Plan to Combat Cybercrime

The RCMP Action Plan to Combat Cybercrime builds on the operational framework. It sets out 15 action items, including success indicators and timelines, to implement the Cybercrime Operational Framework and improve the RCMP's posture against cybercrime.

Action Item	Success Indicators	Planned Timeline
1. Create a new investigative team dedicated to combat cybercrime. Links to operational framework: **P2; O4; O5; O6; E4**	- Conduct more cybercrime investigations. - Apprehend more cybercriminals. - Disrupt more cybercrime activity.	Ramp-up: 2015-2020. Full implementation: 2020 and ongoing.
Description: The RCMP requires dedicated investigative capacity to address cybercrime, where new technical capabilities are integrated with traditional enforcement measures. To address this requirement, the RCMP will establish a cybercrime team located in Ottawa to **investigate the most significant threats to Canada's political, economic and social integrity that would negatively affect Canada's reputation and economy. The team will have the capacity to target** cyber-related criminal activity targeting the federal government, national critical infrastructure and key business assets. In carrying out its mandate, the team will leverage RCMP operational units across Canada that provide specialized and technological services in support of cybercrime investigations, and will work with domestic and international law enforcement partners on joint force operations. The team will enhance the RCMP's ability to combat cybercrime-related offences where technology plays an integral role, such as investigating the unauthorized use of computers, mischief in relation to data, or the possession of a device to commit unauthorized computer use or data mischief.		
2. Establish a governance structure for cybercrime priorities and operations. Links to operational framework: P1; P2; P3; O3; O6; E3; E4; E5	- Provide governance, oversight and accountability for the cybercrime investigative team. - Provide tactical operational support, advice and direction to all major investigational cybercrime projects.	Ramp-up: 2015-17. Full implementation: 2017 and ongoing.
Description: The RCMP requires a governance structure to oversee cybercrime investigative priorities and operations. To address this requirement, the RCMP will devote personnel to provide governance, oversight and accountability for the new cybercrime investigative team, within the frame of the RCMP's **governance structure for its serious and organized crime, national security and financial crime priorities. The RCMP's cybercrime governance structure will fall under RCMP Federal Policing** Criminal Operations. Other oversight mechanisms will be in place for the RCMP's specialized services that support cybercrime investigations.		

Action Item	Suggested Actions	Planned Timeline
3. Create a dedicated intelligence unit to identify new and emerging cybercrime threats. Links to operational framework: **P1; O1; O2; O3; E3; E4; E5**	- Collect and analyze data sources on cybercrime threats and trends to identify vulnerabilities and enforcement opportunities for investigators. - Produce cybercrime intelligence to identify leads and operational priorities for enforcement action.	Ramp-up: 2015-17. Full implementation: 2017 and ongoing.
Description: The RCMP requires dedicated resources to analyze more data sources and foster a strategic, national intelligence picture of cybercrime, and to better identify major cybercrimes for enforcement action. To address this requirement, the RCMP will establish a dedicated cybercrime intelligence unit **within the RCMP National Intelligence Coordination Centre (NICC). The NICC will gather** and analyze cybercrime intelligence from domestic and international sources where suspected **cybercrime activity has been identified and reported to the RCMP. The dedicated cybercrime** intelligence unit will enhance the RCMP's ability to analyze cybercrime threats in an operational **capacity and direct resources to target Canada's most serious and prolific cybercriminals. The** NICC will also improve the RCMP's ability to link cybercrime threats to criminal activity in other **domains, such as financial crime or serious and organized crime.**		
4. Improve digital evidence capabilities for cybercrime investigations. Links to operational framework: **P3; O7; O8; E2**	- Provide digital forensic support to cybercrime investigations, including those led by the cybercrime investigative team. - Acquire new operational tools to analyze digital evidence more **effectively.**	Ramp-up: 2015-2020. Full implementation: 2020 and ongoing.
Description: Cybercrime investigations differ significantly from traditional criminal investigations. They have a greater requirement for operating in online environments through open source analysis and covert means, and obtaining and analyzing data (potential digital evidence) to drive **investigations. The new cybercrime investigative team is expected to handle large and complex** volumes of digital evidence, such as potential evidence from lawfully seized digital devices and servers. To address this requirement, the RCMP will devote new personnel and acquire new operational tools to directly support digital evidence requirements for cybercrime investigations, including **those led by the new cybercrime investigative team. These digital forensic resources will ensure** that state-of-the-art technological tools and capabilities are in place to support priority cybercrime investigations. In addition, the RCMP will examine capacity and capability requirements to push digital forensic skills and tools to the frontline of policing.		

[illegible]	[illegible]	[illegible]
5. Expand cybercrime investigative training opportunities for Canadian law enforcement Links to operational framework: **P3; O9;** E1	- Develop and implement new cybercrime investigative courses for law enforcement. - Expand basic and advanced cybercrime investigative skills across Canada.	Ramp-up: 2015-17. Full implementation: 2017 and ongoing.
Description: Criminal investigators and intelligence analysts require basic and advanced training in new and emerging technologies to keep pace with cybercrime. To address this requirement, the RCMP will improve its law enforcement training for cybercrime-related matters by providing new cybercrime investigative and intelligence training opportunities for the RCMP and its provincial and municipal law enforcement partners. **The RCMP provides law enforcement training on cybercrime investigative and intelligence-**gathering techniques through the Canadian Police College, Technological Crime Learning Institute **(TCLI). The TCLI is the only institute in Canada that offers a comprehensive cybercrime training program for law enforcement on various cybercrime investigative techniques. Through the TCLI,** the RCMP will develop and implement new courses on digital and mobile device analysis, and Internet-based open source and online covert investigative techniques, areas in high demand from Canadian law enforcement agencies.		
6. Examine ways to more effectively recruit cybercrime investigators and other individuals with technical skills to combat cybercrime. Links to operational framework: P2; P3; O4; O5; O9; E1	- Develop a strategy to more effectively recruit cybercrime investigators, intelligence analysts and other individuals with technical skills to combat cybercrime. - Consider cyber recruitment strategies by other government organizations.	Ongoing.
Description: Cybercrime investigations are often complex, long-running and require individuals **with highly specialized and technical skills, such as advanced proficiencies in computer science** and network engineering, and other technical domain areas. To address this requirement, the RCMP will examine its existing recruitment strategies for police **officers and civilians, and will consider new recruitment tactics to better attract and retain individuals** with technical domain expertise in cyber technologies. Recruitment strategies may include examining international recruitment models and other ways to reform cyber recruitment measures, such as considering: the United States, Department of Homeland Security, Cyber Student Volunteer Initiative; the United Kingdom's Joint Cyber Reserve; developing targeted recruitment campaigns **aimed at academic institutions that specialize in computing or similar technological fields;** promoting immediate cybercrime investigative training opportunities for new RCMP Cadets; or taking part in broader recruitment initiatives within the government's cyber community.		

Action Item	Success Indicators	Planned Timeline
7. Strengthen public-private partnerships and other liaison **efforts in combating cybercrime.** Links to operational framework: **P1; O3; E5**	- More public-private partnerships and liaison channels on operational matters concerning cybercrime. - More data sources on cybercrime threats and trends with links to Canada.	Ongoing.
Description: No single organization holds all of the requisite information to fully comprehend, keep pace with and combat cybercrime. Cybercrime is vast in scope and magnitude, and requires public and private sector organizations to work together and share information on new and emerging cybercrime threats. To address this requirement, the RCMP will continue to expand its public-private partnerships **and liaison efforts in combating cybercrime. The RCMP will build stronger partnerships with key cybercrime-fighting organizations, such as the United States National Cyber-Forensics & Training** Alliance (NCFTA), the NCFTA Canada, and organizations in Canada's critical infrastructure industries to develop a more comprehensive understanding of major cybercrime threats and ways to address them.		
8. Examine ways to enhance the CAFC as a trusted data and **intelligence source on financially-**motivated cybercrimes. Links to operational framework: **P1; O1; O2; O3; E3; E5**	- Analyze and disrupt a wider **spectrum of financially-motivated** cybercrime threats. - Improve victim-based reporting **of financially-motivated** cybercrime incidents.	Ongoing.
Description: The Canadian Anti-Fraud Centre (CAFC) plays an important role in analyzing and mitigating online fraud by working with Canadian police services and industry to disrupt criminal adversaries in cyberspace. Financially-motivated cybercrimes, however, are not limited to fraud, **and require law enforcement to consider other offences.** To address this requirement, the CAFC will examine requirements to address a wider spectrum **of financially-motivated cybercrime threats, such as reported cybercrime incidents involving intellectual property infringements and identity theft. The CAFC will also examine ways to expand** its intake capabilities for victim-based reporting of suspected cybercrime incidents and improve its **police information sharing on cybercrime activities and trends. The RCMP will also examine the** role of the CAFC in the context of Federal Policing's overall intake framework, including potential links to National Police Services.		

Action Item	Sub-Activities	Planned Timelines
9. Examine ways to improve the collection and analysis of suspicious cybercrime incidents involving Canada's critical infrastructure and other vital cyber systems. Links to operational framework: **P1; O1; O2; O3; E3; E5**	- Improve the collection and analysis of suspicious and possibly criminal cyber incidents occurring at critical infrastructure facilities and other vital cyber operations in Canada. - Engage Canada's critical infrastructure and vital cyber systems community to inform of suspected cybercrime threats and ways to address them.	Ongoing.
Description: Cybercrime poses serious threats to Canada's critical infrastructure and other vital cyber systems, such as those in energy, telecommunications and financial sectors. Critical infrastructure systems may include Internet-facing components, potentially leaving them vulnerable to malicious software and other cybercrime threats. The impact of these threats to critical infrastructure and other vital cyber systems may vary, ranging from industrial espionage, to data extraction and theft of intellectual property or trade secrets, to more disruptive tactics involving system compromises. These threats are growing in sophistication and volume, and require greater collaboration between law enforcement and other public and private sector stakeholders. To address this requirement, the RCMP will examine ways to improve its collection and analysis of suspicious cybercrime incidents involving Canada's critical infrastructure and other vital cyber systems. This initiative will consider the RCMP National Critical Infrastructure Team (NCIT) and its analysis of cybercrime threats to critical infrastructure and other vital cyber systems. This initiative will also involve law enforcement collaboration with Canada's critical infrastructure community, such as the National Cross Sector Forum and sector-specific briefings. Notably, the NCIT examines physical and cyber threats to Canada's critical infrastructure, and collaborates with law enforcement, public and private sector stakeholders to ensure a common understanding of the criminal threats and risks surrounding Canada's critical infrastructure, including those in the cyber realm.		
10. Improve the intake and triage of reported cybercrime incidents. Links to operational framework: **P1; O1; O2; O3; E3; E5**	- Improve ability to obtain and disseminate information on cybercrime incidents to operational areas. - Improve situational awareness on suspected cybercrime activity in Canada.	Ongoing.
Description: The RCMP anticipates that domestic and international cybercrime incidents will require a greater ability to intake and triage requests for law enforcement assistance, improve situational awareness on cybercrime activities in Canada and disseminate information on cybercrime incidents to RCMP jurisdictions and other Canadian police services. To address this requirement, the RCMP will examine ways to improve its intake and triage functions for reported incidents of suspected cybercrime activities. This initiative will focus on examining RCMP operational areas that facilitate intake and triage functions for domestic criminal investigations and foreign law enforcement requests for assistance, including the RCMP Federal Policing Operational Information Management Intake Unit and INTERPOL Ottawa.		

The RCMP will also examine its international networks involving reported cybercrime incidents and foreign requests for law enforcement assistance, including INTERPOL, G7 and the Council of Europe's Convention on Cybercrime 24/7 networks. More broadly, the RCMP, through Federal Policing and National Police Services, will examine how it can better assist all Canadian law enforcement to intake and triage new cybercrime complaints and coordinate cybercrime investigations involving the widespread unauthorized use of computers and mischief in relation to data.		
Action Item	Success Indicators	Planned Timeline
11. Examine integrated enforcement models for combating cybercrime. Links to operational framework: **P1; P2; O3; O6; E4**	- Greater national coordination **and deconfliction for major** cybercrime investigations.	Ongoing.
Description: Cybercrime activities are often multi-jurisdictional in nature and require the **combined efforts of Canadian police services, including national law enforcement coordination and deconfliction.** To address this requirement, the RCMP will examine its existing enforcement models for joint force operations and will consider models that may better address criminal investigations in the cyber realm. An emphasis will be placed on examining national law enforcement coordination and **deconfliction measures for technically complex and multi-jurisdictional cybercrimes, particularly** those involving the widespread unauthorized use of computers and mischief in relation to data. **This examination will focus on examining operations across RCMP federal policing, contract** policing and national police services, including protocols for collaboration between the RCMP and its provincial and municipal law enforcement partners.		
12. Expand international collaboration with close allies to better understand and combat cybercrimes that are transnational in character. Links to operational framework: **P1; P2; O3; O6; E4**	- Greater participation in international law enforcement fora on cybercrime. - Greater understanding of cybercrime threats that are transnational in character. - **Provide liaison officers and** analysts deployed abroad with foundational cyber-related training as it becomes available.	Ongoing.
Description: Cybercrime is often an international threat that requires an international and cohesive law enforcement response. To address this requirement, the RCMP and its international law enforcement allies are increasingly working together to develop a shared understanding of common cybercrime threats, and to ensure that collaborative, proactive operational activities are aligned against these threats. **Through key international bodies, such as INTERPOL, EUROPOL, G7 and Five Eyes working** groups, the RCMP will continue to work with its international law enforcement allies to identify and address common cybercrime threats.		

The RCMP will also examine ways to bolster its international role in combating cybercrime, such as playing more active and leadership roles in shared international threat assessments and **prioritization activities against cybercrime. This work may include international law enforcement** activities involving the RCMP, such as: the Five Eyes Law Enforcement Group, Cyber Crime Working Group; the Europol's Cyber Crime Centre, Joint Cybercrime Taskforce; the G7 Roma Lyon Group, High-Tech Crime Subgroup; the NCFTA International Task Force; and the INTERPOL Global Complex for Innovation.

Action Item	Specific Objectives	Planned Timeline
13. Examine ways to further inform Canadians and industry of emerging cybercrime threats. Links to operational framework: P1; O1; O2; O3; E3; E6	- Provide Canadians and industry with more relevant and timely information on cybercrime threats. - Encourage Canadians and industry to take proactive measures against cybercrime.	Ongoing.
Description: Under the broad context of cyber security, public and private sector organizations, **and Canadians themselves, play important roles in addressing cybercrime. The private sector** has a critical cyber role in securing its own networks and systems of wider importance, such as telecommunications, banking and other critical infrastructure sectors. Canadians should also take basic measures to protect themselves online, such as using up-to-date cyber security and anti-virus software, using unique and secure user names and passwords, and downloading online applications from only trusted sources. To take these and other proactive measures against cyber threats, Canadians and industry must be aware of cybercrimes facing Canada. To address this requirement, the RCMP will continue to work with Public Safety Canada and other organizations by informing Canadians and industry of new and emerging cybercrime threats. Notably, the RCMP National Crime Prevention Services assist with public awareness and educational strategies to prevent cyber bullying, including initiatives related to Public Safety Canada's *GetCyberSafe* **campaigns. The RCMP will continue to support the** *GetCyberSafe* **campaigns through youth crime prevention activities. The RCMP will also look for ways to** increase industry's awareness of emerging cybercrime threats through the Canadian Association of Chiefs of Police, Private Sector Liaison Committee, and improved information-sharing between the RCMP National Critical Infrastructure Team and critical infrastructure owners and operators.		
14. Continue to support the modernization of Canada's legal and policy tools to keep pace with technological change. Links to operational framework: P2; O6; E7	- Modernized and new criminal **offences and investigative legal** tools to better address cybercrime in Canada. - Improve law enforcement's ability to conduct international cybercrime investigations through harmonized legal tools between state allies.	Ongoing.

Description: At all levels of government, the RCMP and other Canadian police forces address cybercrime within the boundaries of Canada's legal environment, which includes a combination of jurisprudence, legislation, public policies, and other legal and policy instruments. While the RCMP Cybercrime Strategy focuses on strengthening the RCMP's posture against cybercrime within today's legal environment, it is clear that Canada's legal and public policy regime will need to keep pace with **the evolution of technology to permit the effective investigation of cybercrime, both domestically and** internationally.

The RCMP will continue to support Canada's modernization of criminal offences and investigative tools to better address crime in a digital age. The RCMP will also engage Canada's criminal justice community and identify requirements for educating prosecutors on cybercrime investigations and the novel legal aspects of cybercrime.

Action Item	Success Indicators	Planned Timeline
15. Continue to work with the broader Canadian law enforcement community to devise a 'national' picture of - and response to - cybercrime. Links to operational framework: P2; O6; E4	- Provide a leadership role in developing a framework for a 'national' law enforcement strategy to combat cybercrime. - Identify actions that could be taken by all Canadian police **forces to more effectively address** cybercrime.	Ongoing.

Description: Cybercrime represents a shared and common threat to all levels of policing in Canada, and requires collaboration between the RCMP and its Canadian law enforcement partners.

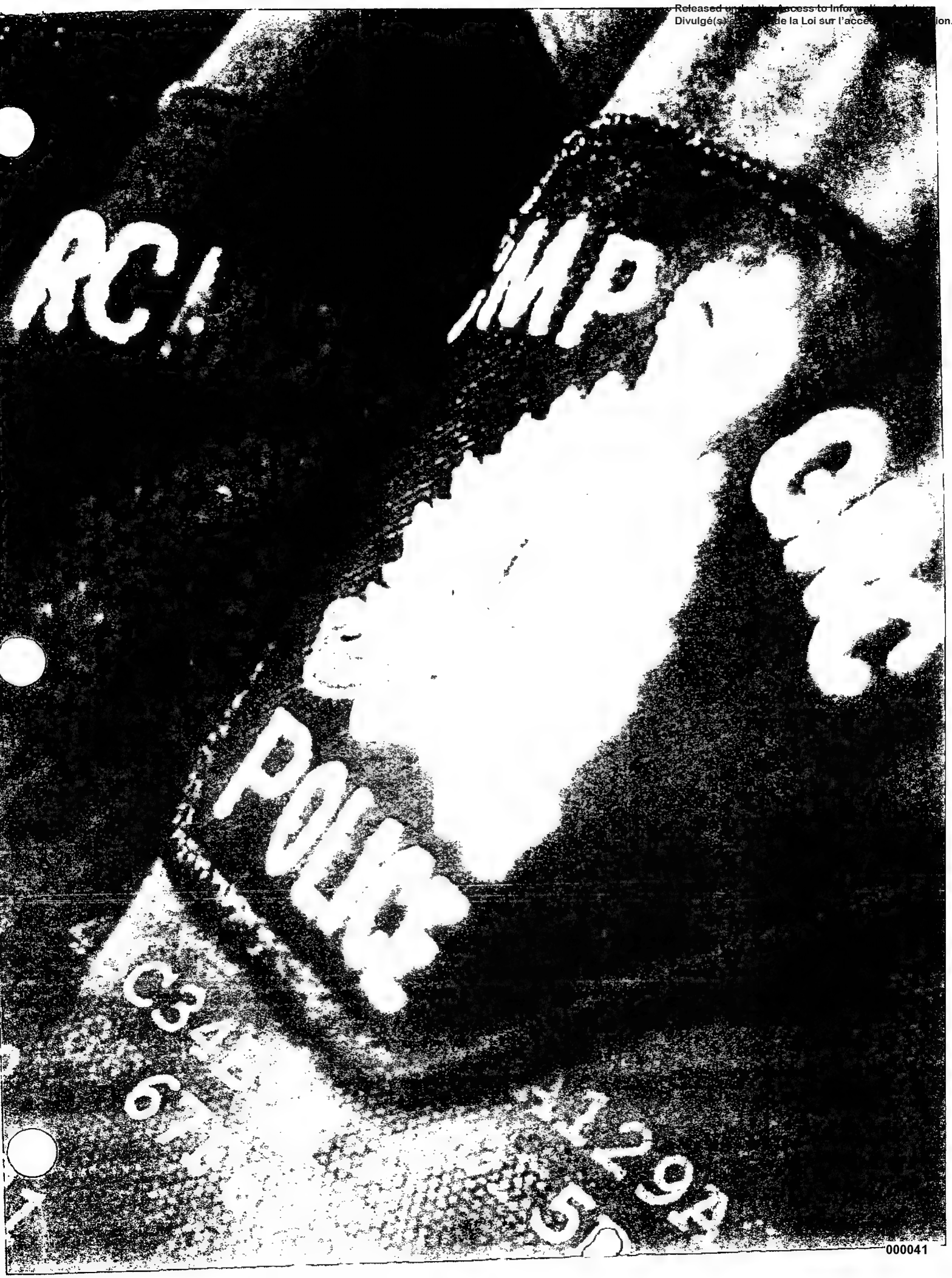
To address this requirement, the RCMP and its Canadian law enforcement partners, through the Canadian Association of Chiefs of Police, Electronic Crime Committee, and other fora, continue to discuss and develop coordinated, national law enforcement approaches to combat cybercrime. Consistent with this approach, the RCMP will use the RCMP Cybercrime Strategy as a basis to lead the development of broader national law enforcement strategies against cybercrime, including measures to develop a broader account of cybercrime based on aggregated police data, and to identify and improve shared, multi-jurisdictional law enforcement operations, collaboration and **deconfliction measures against cybercrime. The RCMP will also engage other key stakeholders,** such as the National Police Services National Advisory Committee and the Five Eyes Law Enforcement Group, Cyber Crime Working Group, to fully examine operational requirements for a national law enforcement strategy to combat cybercrime.

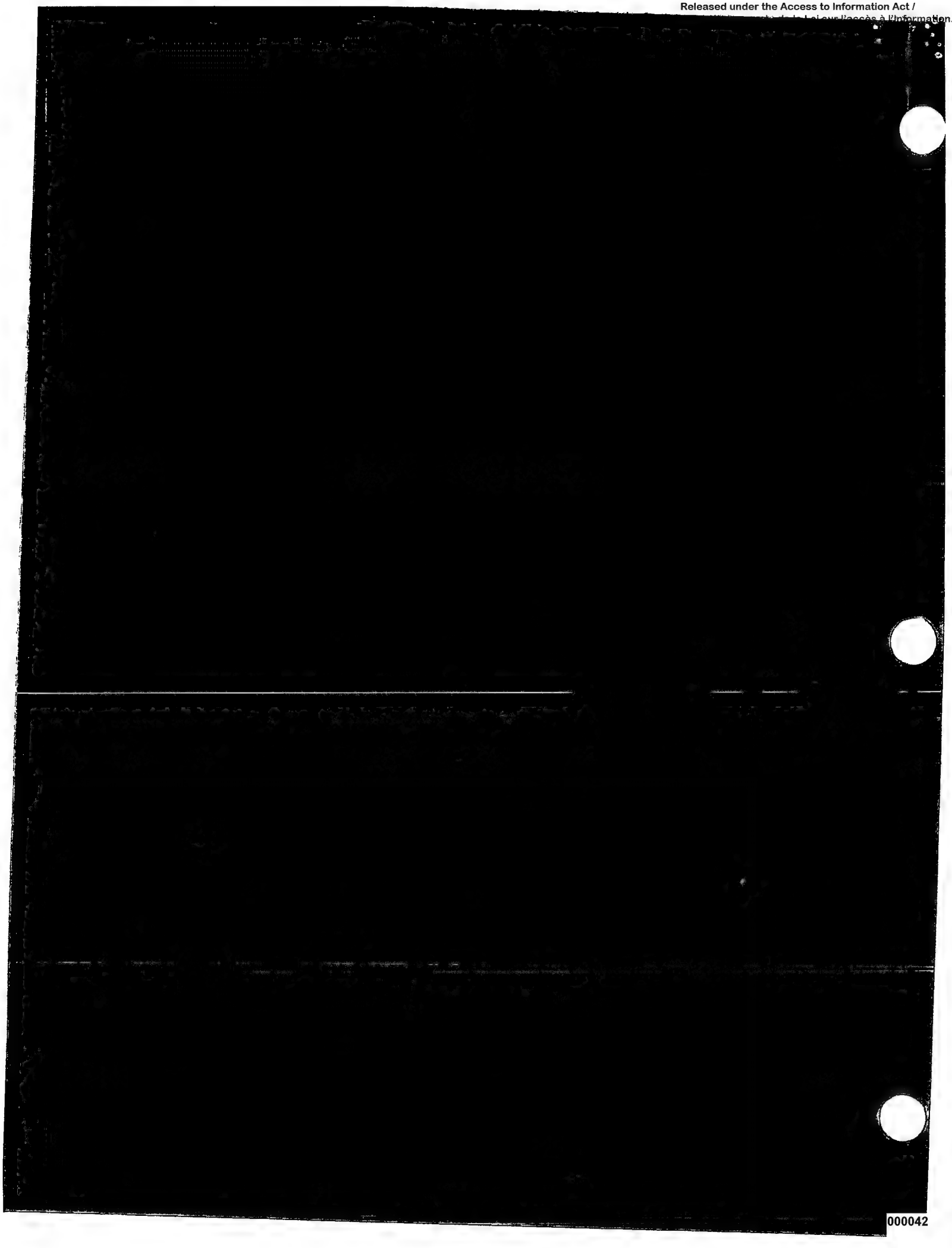
Conclusion

Cybercrime has an immediate, tangible and ongoing impact on Canadians. On a macro level, cybercrime affects Canadian government and critical infrastructure systems and the integrity of Canada's economy and financial sectors. On a personal level, cybercrime involves personal financial losses, the infringement of privacy rights and the grievous harm associated with offences such as child sexual exploitation and cyber bullying. These threats continue to evolve and require a paradigm shift in how crimes are understood and policed in a digital era. They require a law enforcement response that addresses the criminal element in cyberspace while complementing broader government and industry security measures.

The *RCMP Cybercrime Strategy* identifies key steps that Canada's national police force will take to address this challenge. The strategy's action items are operationally relevant and will enable the RCMP to more effectively keep pace with cybercrime. The RCMP's cyber deliverables will be measured and reported on through *Canada's Cyber Security Strategy*.

The *RCMP Cybercrime Strategy* will strengthen the RCMP's ability to work with its domestic and international law enforcement partners and other stakeholders to combat cybercrime.





Public Safety Canada / Sécurité publique Canada

ANNEX C

BUILDING A **SAFE** AND **RESILIENT CANADA**

Update on Recent Cyber Security Developments

Deputy Ministers Committee on Cyber Security

January 26 2016

Canada

Government of Canada Systems

- Cyber Security Emergency Management Plan (CSEMP)
  - GC CIO announced CSEMP v1.4 is to be followed - effective August 4, 2015
  - Invoked proactively to support Elections Canada during election period – operation very successful test of CSEMP
- DDoS incident – Summer 2015
  - Targeted security and intelligence agencies
  - Lessons Learned process ongoing
- Phishing attempts from state sponsored actors
  - More attempts in first half of 2015 than all of 2014
- Multiple large scale compromises of personal information databases
  - OPM, Ashley Madison, TalkTalk
  - S&I community to re-examine risks of outsourcing the management of aggregate info about GC personnel to external service providers
- GC Cloud Computing Strategy Consultation
  - Public Sector CIO Council approved the Public Sector Secure Community Cloud vision and work plan

- Standard on Security Screening – Application for Judicial Review
  - Key safeguard for mitigating the "insider threat" to GC cyber security
  - Federal Court dismissed a motion for judicial review of the Standard
    - Applicants failed to prove irreparable harm (to both union members and the public good) if the Standard is implemented

- Office of the Comptroller General Horizontal Audit of IT Security
  - High level findings:
    - Opportunities were identified to enhance governance frameworks at the GC level to reflect an enterprise approach for IT security
    - Most departments had some degree of governance framework in place, but room for improvement exists
    - The control frameworks examined within the audit were generally not consistently implemented across the departments and within the GC enterprise infrastructure

Cyber Activity Affecting Canadian Infrastructure

- National cross sector forum commitment to identify CI cyber dependencies:
  - Status: CI cyber dependencies analysis has been completed and lead federal departments and agencies have been consulted
  - Next steps: review analysis with CI sector network representatives

- Usual 5 report outlining 30 high risk vulnerabilities being exploited to target CI organizations

- The G7 Finance Ministers have endorsed the creation of a WG on cyber security in the financial sector

Policy Developments

- Medium term planning around cyber security
  - Deputy Ministers meeting on the Internet in September
- CEO Advisory Committee on Cyber Security
  - Debrief on July 22, 2015 meeting
  - Next meeting tentatively scheduled for February 19, 2015 in TO
  - Canadian Cyber Threat Exchange (CCTX)
- FPT DM Table on Cyber Security
  - Action Plan for discussion
  - Next meeting in early 2016
- Canadian Association of the Chiefs of Police Cybercrime Resolution

s.21(1)(a)
s.21(1)(b)

[redacted]

International Developments and Conferences

- Ratification of the Council of Europe Convention on Cybercrime (Budapest Convention)

s.21(1)(a)
s.21(1)(b)

[redacted]

- China - Bilateral cyber agreements with US & UK
- Invalidation of the Safe Harbour Agreement
- Notable international cyber events (June 2015-December 2015)
  - Ottawa 5, Wellington, NZ, June 8-9
  - Code of Conduct, Russia, July 9-10
  - Seoul Defence Dialogue, September 9-11
  - Internet Governance Forum, Brazil, November 10-13
  - G20, Turkey, November 15-16
  - WSIS+10 - negotiations ongoing until high level meeting, New York, December 15-16

Media Environment

- Themes for cyber security awareness month (October):
  - General cyber security awareness
  - Creating a culture of cyber security at work
  - Connected communities: staying protected while always connected
  - Your evolving digital life
  - Building the next generation of cyber professionals

Pages 50 to / à 51

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 52 to / à 55

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (c)

of the Access to Information Act

de la Loi sur l'accès à l'information